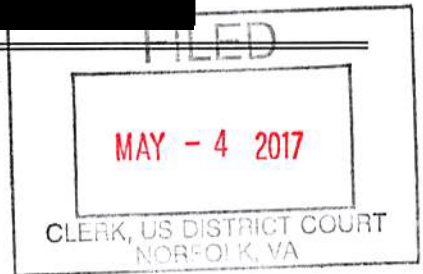


UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia



In the Matter of the Search of)
One (1) 8 GB Micro SD Card located on)
the premises of the HSI Office at)
200 Granby Street, Suite 600 Norfolk, VA 23510)

Case No. 2:17sw 62

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

8 GB Micro SD Card described in Attachment A

located in the Eastern District of Virginia, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)

18 U.S.C. 2252A(a)(5)(B)

Offense Description

Knowingly possesses, or knowingly accesses with intent to view, any media or material that contains an image of child pornography that has been transported through interstate or foreign commerce by any means.

18 U.S.C. § 2422(b)

Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be punished.

The application is based on these facts: **See Affidavit.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

Randy C. Stoker
Assistant United States Attorney

Applicant's signature
Kristin B. Joseph, Special Agent (HSI)
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/4/17
City and state: Norfolk, VA

Judge's signature
Douglas E. Miller
United States Magistrate Judge
Printed name and title

ATTACHMENT A

DESCRIPTION OF THE ITEMS TO BE SEARCHED

The following item was turned over to an HSI Special Agent by the wife of Larry RADEBAUGH and is currently located at the HSI Office at 200 Granby Street, Suite 600, Norfolk, Virginia 23510

- a) 8 GB Micro SD Card

Handwritten signature and initials in blue ink, located in the bottom right corner of the page. The signature appears to be "KBS" with a checkmark above it.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

The following items to be seized constitute evidence of violations of Title 18, United States Code, Sections 2422(b), and 18 U.S.C. 2252A(a)(5)(B), which may be found in the item listed in Attachment A

- a. Materials depicting or containing child pornography, as defined in Title 18, United States Code, Section 2256.
- b. Any record or document pertaining to the possession, receipt, distribution and/or reproduction of child pornography, as defined in Title 18, United States Code, Section 2256.
- c. Any record or document identifying persons transmitting, through interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- d. Any record or document bearing on the production, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- e. Any record or document pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- f. Any record or document which lists names and addresses of any minor visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- g. Any record or document which shows the offer to transmit through interstate commerce any depictions of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- h. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. "Child erotica" may also include, in this context, sex aids and/or toys.

i. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with a minor that are sexually explicit in nature, as defined in Title 18, United States Code, Section 2256.

j. Any documents, records, programs, or applications that identify the residents of the SUBJECT ITEM.

ownership (KBS) Jan

k. Any documents, records, programs or applications that identify the Internet service provided to the SUBJECT ITEM.

l. Any documents, records, programs, or applications tending to demonstrate the actual user(s) of computers found at the SUBJECT ITEM.

(KBS) Jan

(KBS) Jan

FILED
MAY - 4 2017

ACT

CLERK, US DISTRICT COURT
NORFOLK, VA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH)
OF:)

a) 8 GB Micro SD Card)

) Case No. 2:17sw 62
)
)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kristin B. Joseph, being first duly sworn state:

1. I am a Special Agent of the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), currently assigned to the Office of the Assistant Special Agent in Charge (ASAC), Norfolk, Virginia. I have been so employed since August 2005. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography¹ (as defined in 18 U.S.C. § 2256(8)) in all forms of media including computer media. I am also a certified forensic computer examiner for HSI.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for a **8 GB Micro SD Card** located at the HSI Office at 200 Granby Street, Suite 600, Norfolk, VA 23510 (the SUBJECT ITEM), described in Attachment A, for the items specified in Attachment B hereto.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2422(b), and 2252A(a)(5)(B) is located on the SUBJECT ITEM.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2422(b), which prohibits a person from using the

¹ I use the terms "child pornography" and "visual depictions/images of minors engaging in sexually explicit conduct" interchangeably in this Affidavit.

means of interstate or foreign commerce to persuade, induce, entice, or coerce a minor into sexual activity. As well as violations of 18 U.S.C. § 2252A(a)(5)(B), which prohibits a person from knowingly possesses, or knowingly accesses with intent to view, any media or material that contains an image of child pornography that has been transported through interstate or foreign commerce by any means.

PERTINENT FEDERAL CRIMINAL STATUTES

6. 18 U.S.C. § 2422(b) provides that any person who, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be punished.

7. Virginia Code § 18.2-374.1 provides that any person who accosts, entices or solicits a person less than 18 years of age with intent to induce or force such person to perform in or be a subject of child pornography, or produces or makes or attempts or prepares to produce or make child pornography; or who knowingly takes part in or participates in the filming, photographing, or other production of child pornography by any means; or knowingly finances or attempts or prepares to finance child pornography, shall be punished.

8. 18 U.S.C. § 2252A(a)(5)(B), provides that any person who knowingly possesses, or knowingly accesses with intent to view any media or material that contains an image of child pornography that has been transported through interstate or foreign commerce by any means or that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means including by computer shall be punished.

DEFINITIONS

9. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

10. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

11. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of

electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

12. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

13. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

14. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

15. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

16. “Internet Protocol Address” (IP Address), as used herein, refers to refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

17. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

18. "Minor" and "sexually explicit conduct" are defined in 18 U.S.C. §§ 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

- a. Sexual intercourse, including genital on genital, oral genital, anal genital, or oral anal, whether between persons of the same or opposite sex;
- b. Bestiality;
- c. Masturbation;
- d. Sadistic or masochistic abuse; or
- e. Lascivious exhibition of the genitals or pubic area of any person.

19. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

20. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

21. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

22. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

23. The term "Universal Resource Locator" (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

24. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards,

cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

25. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband,

evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

- a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and
- b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

26. Additionally, based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or an unsecured wireless network in their residence are often among the primary users of that wireless network.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

27. Based upon my training and experience and information officially supplied to me by other law enforcement officers, I know the following:

- a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 64 gigabytes of data or more, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.
- c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte (1,000 GB's) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to

save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

- e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.
- g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND INFORMATION ON KIK

28. According to the website <http://KIK.com/about>, KIK advertises itself as “the first smartphone messenger with a built-in browser.” KIK Messenger allows its users to “talk to your friends and browse and share any web site with your friends on KIK.” KIK believes it is at the forefront of the “new era of the mobile web.” KIK was founded in 2009 by a group of University of Waterloo students who started a company designed to “shift the center of computing from the PC to the phone.” KIK Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, KIK usernames - not phone numbers - are the basis for KIK user accounts, so KIK users are in complete control with whom they communicate. In addition, KIK features include more than instant messaging. KIK users can exchange images, videos, sketches, stickers and even more with mobile web pages.

PROBABLE CAUSE TO SEARCH THE SUBJECT ITEM

29. In March 2015, HSI Agents in Louisiana, along with other state and local law enforcement, executed a search warrant at the residence of an individual (hereinafter referred to as MW) suspected of producing child pornography by enticing minor females into sending him images and videos of themselves using the chat application KIK. Among the items seized pursuant to the search warrant was a cellular phone. Forensic analysis of this cell phone revealed that MW used KIK to extort and solicit images of suspected minor females, as well as to discuss and trade images of minor females with other KIK users. MW was using the persona of a juvenile female to initially be-friend other juvenile females. One of the chats discovered was between MW and another KIK user with the username "gfy02."

30. The chat indicated that "gfy02" initially believed that MW was a juvenile female and he was possibly going to attempt to entice MW into sending nude pictures. The user of "gfy02" even threatened MW that he was going to "*post you*" because MW was not responding to the requests. Throughout the chat, MW revealed to "gfy02" that he was using a fake persona. Their discussions eventually lead to "gfy02" asking MW to trade images of child pornography.

31. In April 2015, KIK responded to an HSI summons for subscriber information for "gfy02." The user provided a first name of "Anthony" and an e-mail address of dakotadude002@gmail.com. The user account initially was registered on 02/28/2015. Additionally, KIK provided IP log information for the user "gfy02" which indicated that the account was most frequently accessed between 03/09/2015 and 04/10/2015 from a wireless Internet account using the IP Address of 173.71.153.142.

32. Verizon, the owner of the latter IP Address, responded to an HSI administrative summons and reported the following subscriber was assigned the IP address 173.71.153.142: Larry Anthony RADEBAUGH at his residence in Virginia Beach.

33. HSI issued an administrative summons to Google, Inc. for subscriber information for the e-mail accounts dakotadude002@gmail.com. On August 01, 2016, Google, Inc. responded to the summons and provided the subscriber information for dakotadude002@gmail.com. The name provided to Google was Anthony Smith and the account was created on 09/24/2014. Additionally, Google provided IP login information for dakotadude002@gmail.com, which indicated that the account was most frequently accessed between 01/29/2016 and 07/29/2016 from a wireless Internet account using the IP address of 71.120.236.197.

34. Verizon, the owner of the latter IP Address, responded to an HSI administrative summons and reported the following subscriber was assigned the IP address 71.120.236.197: Larry Anthony Radebaugh at his residence in Virginia Beach.

35. On February 13, 2017, HSI Norfolk special agents conducted an interview of Larry Anthony Radebaugh at this residence in Virginia Beach. During this interview, RADEBAUGH admitted to using the application KIK and other applications to chat online. He stated he received pictures of child pornography on KIK by means of Dropbox (an online cloud storage company) links, but he deleted it and never sought it out. He admitted he used to use the "gfy02" username but he no longer used it. He stated he created a new KIK username of

“fml03.” Also during the interview, RADEBAUGH admitted to using another texting application called TextNow. RADEBAUGH confirmed that he used the e-mail accounts dakotadude002@gmail.com and gfy0069@gmail.com.

36. RADEBAUGH gave Agents consent to view his cellular phone and provided the passcode. Law enforcement reviewed some of the applications with RADEBAUGH and asked him about the people he chatted with using the application TextNow. RADEBAUGH responded that the phone number 606-***-**** belongs to “Jane Doe 1” and she is 15 years old. Furthermore, RADEBAUGH explained that he initially met Jane Doe 1 through KIK but shifted to talking on TextNow.

37. RADEBAUGH is 41 years old.

38. Agents transported RADEBAUGH’s cell phone, a Samsung Galaxy that was manufactured outside of Virginia, back to the HSI Office in Norfolk for further analysis. An HSI Computer Forensic Analyst (CFA) performed an extraction using Cellebrite Mobile Forensic Software. The forensic examination of the cell phone revealed numerous chats that appear to be sexual in nature on various different applications, such as KIK and TextNow.

39. In most of the chats, the two parties seemed already familiar with one another indicating that they have been chatting for an extended period. One such chat using the TextNow application is with “Jane Doe 1” from telephone number 606-939-****. In this chat, Jane Doe 1 refers to the other person as “Anthony.” Excerpts from the chats are described below:

On February 5, 2017 at 3:43:12 AM (UTC-5)

RADEBAUGH:	Can I see your pussy
Jane Doe 1:	I need to shave
RADEBAUGH:	Its ok
RADEBAUGH:	I still want to see
Jane Doe 1:	You sure
RADEBAUGH:	Yep
Jane Doe 1:	I can go shave
RADEBAUGH:	Depends how long
Jane Doe 1:	Idk [I don't know]
RADEBAUGH:	ok
Jane Doe 1:	okay
RADEBAUGH:	ok
Jane Doe 1:	ok
RADEBAUGH:	ok
Jane Doe 1:	So
RADEBAUGH:	Are you gonna

Jane Doe 1: What
 RADEBAUGH: Show me
 Jane Doe 1: You sure
 RADEBAUGH: Ya
 Jane Doe 1: ok
 RADEBAUGH: Guess not
 Jane Doe 1: What
 RADEBAGH: Pussy
 Jane Doe 1: Oh
 RADEBAUGH: Do you wanna hear daddy cum baby girl
 Jane Doe 1: Oh my damn
 RADEBAUGH: Call me
 RADEBAUGH: Baby
 Jane Doe 1: It's okay babe

40. TextNow, along with KIK, requires the use of the Internet. The Internet is an interconnected network of computers with which one communicates when on-line, and that network crosses state and national borders.

41. Further analysis of the chats on RADEBAUGH's phone revealed an additional KIK username which was not known to the Agents during the interview. RADEBAUGH provided "fml03," but an additional username of "fml04" was also discovered on his phone and was involved in chats with suspected juveniles.

42. HSI issued an administrative summons to KIK for IP log information. KIK's response indicated that the username "fml04" was accessed multiple times after the HSI Agents left RADEBAUGH's residence. Specifically, the user accessed the account from February 13, 2017, through February 15, 2017. Also, the IP access logs for both usernames "fml03" and "fml04" were accessed from the same wireless IP address of 71.120.236.197.

43. Also during the interview, RADEBAUGH gave Agents consent to access his online accounts such as his e-mail and Dropbox. After the interview, agents accessed RADEBAUGH's Dropbox account from the HSI Norfolk office and observed multiple folders entitled with girls' names. Each folder contained numerous, sometimes hundreds, of images and videos of suspected juveniles posing nude and engaging in sexually explicit activity. An HSI Agent changed the password to the account so he could access the account at a later date for further review.

44. HSI also accessed the two e-mail accounts, dakotadude002@gmail.com and gfy0069@gmail.com, which RADEBAUGH had provided in connection to his KIK accounts. The passwords to these accounts were changed by HSI as well.

45. On February 23, 2017, an HSI Agent attempted to access RADEBAUGH's Dropbox account using the login name RADEBAUGH provided and the password that was

created by the HSI agent on February 13, 2017. The HSI Agent found that the account was completely empty and all the files had been deleted.

46. The HSI Agent then logged into the gfy0069@gmail.com e-mail account, and within this account was an e-mail from Dropbox dated February 14, 2017. The e-mail stated that a large amount of files had been deleted from the Dropbox account. The e-mail further provided directions on how to recover the deleted files within 30 days. The HSI Agent used those directions and again accessed the Dropbox account. The Agent found a section of the "deleted files" which indicated that over 1,000 files had been deleted on or about February 13, 2017.

47. On February 24, 2017, Larry Anthony Radebaugh was arrested by Virginia Beach Police Department (VBPD), with the assistance of HSI Norfolk, for state violations involving the enticement of a minor, possession of child pornography, and obstruction. RADEBAUGH was transported to the VBPD Headquarters. After being provided his *Miranda* Rights, he consented to be interviewed.

48. RADEBAUGH admitted to having a "relationship" with Jane Doe 1 (referenced *infra*) and that he knew her to be 15 years old. He stated he had been chatting with her for almost 2 years using various communication means such as texting, Skype, and KIK. He stated that he received numerous nude images and videos of her performing sex acts, which are stored in his Dropbox account. He also stated they would use Skype to have "phone sex" and he would watch Jane Doe 1 masturbate and he would sometimes take screenshots of this act while it was happening.

49. I have reviewed the folder entitled "[Jane Doe 's first name]" which was located in RADEBAUGH's Dropbox account. I confirmed that there are over 700 images and over 60 videos of Jane Doe 1 engaged in various stages of sexual conduct such as exposing her breasts and genitals, as well as masturbating.

50. Also during this interview, RADEBAUGH admitted to accessing his DropBox account from an old phone on February 13, 2017, after the HSI Agents left his residence. He stated he deleted the entire contents of his Dropbox because he was scared.

51. On April 28, 2017, RADEBAUGH was arrested pursuant to a Federal Criminal Complaint for violations of 18 U.S.C. § 2422(b) and 18 U.S.C. § 1519. HSI Agents transported him from the Virginia Beach City Jail to the U.S. District Courthouse in Norfolk, VA for his initial appearance.

52. On May 1, 2017, RADEBAUGH's wife, Sarah Radebaugh, called your Affiant and informed that RADEBAUGH had called her house from jail and instructed their minor son to retrieve an 8 GB micro SD card from the garage and to hide it somewhere else. That same day, HSI Agents went to the Radebaugh residence in Virginia Beach, VA to interview Sara Radebaugh and to retrieve the micro SD card. Sara Radebaugh stated that on approximately Wednesday night the week prior, her minor son confessed to her that while she was out of the house, RADEBAUGH called and told him exactly where to retrieve the SD card, and instructed him to hide it somewhere else. RADEBAUGH also told their minor son not to tell his mom.

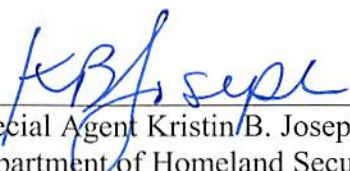
Sara Radebaugh stated that RADEBAUGH didn't want her to know about the SD card because he knew she would tell Agents. She stated that RADEBAUGH was mad at her for previously cooperating with the investigation and telling Agents about the phone she retrieved from his jacket at work.

CONCLUSION

53. Based on the aforementioned factual information, I respectfully submit that probable cause exists to believe that Larry RADEBAUGH is involved with the enticement of a minor to engage in sexually explicit activity, in violation of U.S.C. §§ 2422(b), which prohibits a person from using the means of interstate or foreign commerce to persuade, induce, entice, or coerce a minor into sexual activity. In addition, Larry RADEBAUGH has knowingly possessed, or knowingly accessed with intent to view, any media or material that contains an image of child pornography that has been transported through interstate or foreign commerce by any means.

54. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found within the **8 GB Micro SD Card**. Accordingly, I request that a warrant be issued authorizing me, with assistance from additional HSI agents and other law enforcement personnel, to search the **8 GB Micro SD Card** for the items specified in Attachment B.

FURTHER AFFIANT SAYETH NOT.



Special Agent Kristin B. Joseph
Department of Homeland Security
Homeland Security Investigations
Norfolk, VA

SUBSCRIBED and SWORN before me on this 4th of May 2017.



UNITED STATES MAGISTRATE JUDGE

Douglas E. Miller
United States Magistrate Judge